SOPHOS

Security made simple.

# Sophos Enterprise Console
# Guide de mise à niveau

Version du produit : 5.3.0

Date du document : avril 2015

# Table des matières

1 À propos de ce guide....3
2 À partir de quelles versions puis-je effectuer la mise à niveau ?....4
3 Sophos Disk Encryption....5
3.1 Comment ajouter Sophos Disk Encryption ?....5
4 Quelles sont les étapes de la mise à niveau ?....6
5 Configuration requise....7
5.1 Conditions requises en matière d'espace disque....7
6 De quels comptes avez-vous besoin ?....9
7 Est-ce que je vais bénéficier des mêmes mises à jour qu'auparavant ?....10
7.1 À propos des versions fixes des logiciels....11
7.2 À propos de la mise à niveau de Sophos Update Manager....11
8 Téléchargement du programme d'installation....13
9 Mise à niveau de l'Enterprise Console....14
9.1 Sauvegarde des données et de la configuration de l'Enterprise Console....14
9.2 Mise à niveau de l'Enterprise Console....15
9.3 Renforcement de la sécurité de la base de données....16
9.4 Vérification des stratégies existantes....17
10 Activation de la détection du trafic malveillant....18
11 Annexes....19
11.1 Annexe A : mise à niveau de Sophos Disk Encryption 5.61 vers SafeGuard Enterprise ....19
11.2 Annexe B : installation du logiciel de chiffrement sur les ordinateurs d'extrémité ....19
12 Support technique....27
13 Mentions légales....28

# 1 À propos de ce guide

Ce guide vous explique la procédure de mise à niveau vers la version 5.3.0 de Sophos Enterprise Console et la procédure d'activation de la nouvelle fonction de détection du trafic malveillant.

# 2 À partir de quelles versions puis-je effectuer la mise à niveau ?

Vous pouvez procéder directement à la mise à niveau vers l'Enterprise Console 5.3.0 à partir de :

- Enterprise Console 5.2.2
- Enterprise Console 5.2.1 R2
- Enterprise Console 5.2.1
- Enterprise Console 5.2.0
- Enterprise Console 5.1
- Enterprise Console 5.0

Si vous utilisez la version 4.x de l'Enterprise Console ou la version 4.7 de l'Enterprise Manager, vous allez devoir effectuer la mise à niveau en deux étapes : commencez par vous mettre à niveau vers la version 5.1 de l'Enterprise Console puis procédez à la mise à niveau vers la version 5.3.0 de l'Enterprise Console.

Si vous utilisez la version 4.0.1 ou 4.1 de Sophos Control Center, vous allez devoir effectuer la mise à niveau en deux étapes en suivant l'un des chemins de mise à niveau suivants pris en charge :

- Mise à niveau vers la version 5.1 de l'Enterprise Console puis mise à niveau vers la version 5.3.0 de l'Enterprise Console.
- Mise à niveau vers la version 5.2.2 de l'Enterprise Console puis mise à niveau vers la version 5.3.0 de l'Enterprise Console.

**Remarque :** vous avez également la possibilité d'utiliser Sophos Cloud pour administrer vos ordinateurs. Retrouvez une foire aux questions sur Sophos Cloud dans l'article 119598 de la base de connaissances.

Retrouvez également plus d'informations concernant les différents chemins de mise à niveau dans l'article 119105 de la base de connaissances.

Les programmes d'installation des versions précédentes de l'Enterprise Console sont disponibles sur la page de Téléchargements de Sophos Enterprise Console (http://www.sophos.com/fr-fr/support/downloads/console/sophos-enterprise-console.aspx).

**Remarque :** si vous procédez à la mise à niveau à partir des versions 5.2.1, 5.2.1 R2 ou 5.2.2 de l'Enterprise Console, aucun changement du composant de la base de données n'est nécessaire. Retrouvez plus d'informations dans l'article 121956 de la base de connaissances. Si vous procédez à la mise à niveau à partir d'une version plus ancienne et souhaitez mettre à niveau manuellement les bases de données Sophos en exécutant les scripts d'installation de la base de données, veuillez consulter l'article 116768 de la base de connaissances.

# 3 Sophos Disk Encryption

Aucune mise à niveau de Sophos Disk Encryption 5.61 n'est prévue en raison de son retrait du marché prévu au mois de mars 2016. Si vous utilisez Sophos Disk Encryption et l'administrez à l'aide d'une stratégie de **Chiffrement intégral du disque** dans l'Enterprise Console, vous pouvez continuer à le faire suite à la mise à niveau vers la version 5.3.0 de l'Enterprise Console jusqu'au retrait de Sophos Disk Encryption du marché.

Retrouvez plus d'informations sur la mise à niveau de Sophos Disk Encryption 5.61 vers SafeGuard Enterprise dans l'Annexe A : mise à niveau de Sophos Disk Encryption 5.61 vers SafeGuard Enterprise à la page 19.

Si vous n'utilisiez pas Sophos Disk Encryption avant la mise à niveau vers la version 5.3.0 de l'Enterprise Console, vous pouvez l'ajouter après la mise à niveau si vous le souhaitez. Sachez, toutefois, que Sophos Disk Encryption 5.61 n'est pas compatible avec Windows 8 ou supérieur. Pour utiliser le chiffrement sur Windows 8 et version supérieure, envisagez plutôt d'utiliser SafeGuard Encryption.

## 3.1 Comment ajouter Sophos Disk Encryption ?

Si vous utilisez Sophos Disk Encryption et l'administrez depuis l'Enterprise Console, vous n'avez rien à faire. Sophos Disk Encryption continuera de fonctionner comme avant la mise à niveau.

Si vous n'utilisez pas le chiffrement Sophos mais souhaitez l'ajouter maintenant :

- Si vous procédez à la mise à niveau à partir de l'Enterprise Console 5.1 ou version supérieure, veuillez d'abord vous mettre à niveau vers l'Enterprise Console 5.3.0, puis exécuter de nouveau le programme d'installation de l'Enterprise Console 5.3.0 pour ajouter le chiffrement.
- Si vous procédez à la mise à niveau à partir de l'Enterprise Console 5.0, le programme d'installation va afficher la page **Administration du chiffrement** à partir de laquelle vous allez pouvoir choisir d'administrer le chiffrement (comme décrit à la section Mise à niveau de l'Enterprise Console à la page 15).

Après avoir ajouté le chiffrement, vous allez devoir installé le logiciel de chiffrement sur les ordinateurs d'extrémité comme décrit à la section Annexe B : installation du logiciel de chiffrement sur les ordinateurs d'extrémité à la page 19.

# 4 Quelles sont les étapes de la mise à niveau ?

La mise à niveau comprend les étapes suivantes :

- Vérification de la configuration système requise.
- Vérification des comptes nécessaires.
- Vérification d'une éventuelle possibilité de changer d'abonnements logiciel.
- Téléchargement du programme d'installation.
- Mise à niveau de l'Enterprise Console.

Si votre licence inclut le chiffrement et que vous ne l'avez pas utilisé avant la mise à niveau, vous avez la possibilité de configurer le logiciel de chiffrement sur les ordinateurs d'extrémité suite à la mise à niveau de l'Enterprise Console.

# 5 Configuration requise

### .NET Framework 4.0

Le programme d'installation de l'Enterprise Console 5.3.0 installe .NET Framework 4.0 sauf s'il est déjà installé.

**Important :** dans le cadre de l'installation de .NET Framework 4.0, certains services système (tel que le Service d'administration IIS) vont redémarrer.

Après l'installation de .NET Framework 4.0, vous allez voir un message vous demandant de redémarrer votre ordinateur. Si vous acceptez, nous vous conseillons de redémarrer l'ordinateur immédiatement ou juste après l'installation.

Retrouvez une liste complète des configurations requises sur le site Web de Sophos http://www.sophos.com/fr-fr/products/all-system-requirements.aspx.

**Info :** vous pouvez exécuter le programme d'installation de l'Enterprise Console pour vérifier si votre système répond aux conditions requises pour la mise à niveau, même si vous ne voulez pas procéder immédiatement à la mise à niveau. Vous pouvez voir les résultats de la vérification du système sur la page **Vérifications de la propriété du système** de l'assistant d'installation. Après avoir examiné les résultats, cliquez sur **Annuler** pour fermer l'assistant. Retrouvez plus d'informations sur les résultats de la vérification du système sur http://www.sophos.com/fr-fr/support/knowledgebase/113945.aspx.

## 5.1 Conditions requises en matière d'espace disque

La quantité d'espace disque dont vous avez besoin pour mettre à niveau l'Enterprise Console dépend de la taille des fichiers de base de données Enterprise Console (fichiers .mdf) et des fichiers journaux de transaction (fichiers .ldf) en cours d'utilisation.

**Info :** les noms des fichiers commencent par « SOPHOS » et contiennent généralement le numéro de version de l'Enterprise Console.

Retrouvez plus d'informations sur les noms de fichiers de base de données pour les différentes versions de la console et sur la manière de retrouver les fichiers de base de données sur disque dans l'article 17323 de la base de connaissances du support (http://www.sophos.com/fr-fr/support/knowledgebase/17323.aspx).

Pour être sûr de disposer d'un espace disque suffisant pour la mise à niveau de l'Enterprise Console :

- Vérifiez le lecteur de disque sur lequel les fichiers de base de données (fichiers .mdf) sont déployés et assurez-vous qu'il dispose d'un espace libre équivalent à au moins trois fois la taille actuelle des fichiers .mdf.
- Vérifiez le lecteur de disque sur lequel les fichiers de transaction (fichiers .ldf) sont déployés et assurez-vous qu'il dispose d'un espace libre équivalent à au moins huit fois la taille actuelle des fichiers de base de données (fichiers .mdf).
- Si les fichiers .mdf et .ldf sont déployés sur le même disque, assurez-vous que celui-ci dispose d'un espace libre équivalent à au moins 10 fois la taille actuelle des fichiers .mdf.

Si vous avez mis à niveau l'Enterprise Console par le passé, vous avez peut-être encore d'anciennes bases de données Enterprise Console qui ne sont plus nécessaires. Pensez à supprimer ces bases de données pour libérer de l'espace disque. Retrouvez plus d'informations

dans l'article 17508 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/17508.aspx).

# 6 De quels comptes avez-vous besoin ?

## Comptes nécessaires pour effectuer la mise à niveau

Assurez-vous que l'utilisateur connecté et effectuant la mise à niveau sur le serveur d'administration dispose des droits suffisants sur toutes les bases de données Sophos. L'utilisateur effectuant la mise à niveau du serveur d'administration doit être membre du rôle « db_owner » sur chaque base de données Sophos (les membres du rôle serveur « sysadmin » disposent des droits suffisants sur toutes les bases de données). Ces droits sont uniquement requis temporairement pendant la mise à niveau. Ils servent à vérifier que les nouvelles bases de données ont été créées et à migrer les données.

**Remarque :** retrouvez une liste des noms de base de données par version de la console dans l'article 17323 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/17323.aspx).

## Compte de base de données Sophos

Lorsque vous procédez à la mise à niveau de votre console d'administration, il se peut que les détails du compte de la base de données vous soient demandés. Ceci arrive lorsque votre compte actuel ne remplit pas les conditions requises.

Votre compte doit :

- Pouvoir se connecter à l'ordinateur sur lequel est installée la console d'administration. Pour les installations distribuées de l'Enterprise Console, le compte doit pouvoir se connecter à l'ordinateur sur lequel le composant Sophos Management Server est installé.
- Pouvoir lire et écrire sur le répertoire temporaire du système, par exemple : « \windows\temp\ ». Par défaut, les membres du groupe « Utilisateurs » disposent de ce droit.
- Avoir un nom d'utilisateur principal (UPN, User Principal Name) associé au compte s'il s'agit d'un compte de domaine.

Tous les autres droits et abonnements de groupes requis par le compte sont attribués automatiquement au cours de la mise à niveau.

Sophos vous conseille d'utiliser un compte qui :

- Ne soit pas paramétré pour expirer et qui n'a aucune limite de connexion.
- Ne soit pas un compte administratif.
- Ne doit pas être modifié suite à la mise à niveau.

Retrouvez plus d'informations dans l'article 113954 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/113954.aspx).

# 7 Est-ce que je vais bénéficier des mêmes mises à jour qu'auparavant ?

À partir de la version 5.2.1, l'Enterprise Console prend en charge de nouvelles options permettant de bénéficier des mises à jour automatiques depuis Sophos. En revanche, elle ne prend pas en charge certaines options plus anciennes. Si vous procédez à la mise à niveau à partir d'une version antérieure et selon les packages logiciels que vous avez sélectionnés lors de l'installation de l'Enterprise Console, il se peut que vous deviez modifier les paramètres de votre abonnement logiciels avant de procéder à la mise à niveau.

Pour ouvrir un abonnement logiciels pour un ordinateur d'extrémité, dans le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**. Dans le volet **Abonnements logiciels**, cliquez deux fois sur l'abonnement que vous voulez vérifier.

Pour ouvrir un abonnement logiciels du gestionnaire de mise à jour, allez dans la vue **Gestionnaires de mise à jour** et cliquez deux fois sur le gestionnaire de mise à jour que vous voulez vérifier. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, choisissez l'onglet **Avancés**.

Le tableau ci-dessous vous indique si vous pouvez ou non procéder à la mise à niveau avec vos paramètres actuels.

| Package logiciels | Mise à niveau possible | Conseil (si nécessaire) |
|---|---|---|
| ***Ordinateur d'extrémité*** | | |
| Recommended (par défaut) | Oui | |
| Previous | Oui | |
| Oldest | Non | Veuillez-vous réabonner à un package différent (par exemple « Previous »). |
| Extended Maintenance Recommended | Oui | |
| Extended Maintenance Previous | Oui | |
| Extended Maintenance Oldest | Non | Veuillez-vous réabonner à un package différent (par exemple « Extended Maintenance Previous »). |
| Fixed (par exemple : *10.3.11.2 VE3.53.0*) | Oui | Aucune action n'est requise de votre part pour le moment. Retrouvez plus d'informations à la section À propos des versions fixes des logiciels à la page 11. |
| ***Gestionnaire de mise à jour*** | | |
| 1 Recommended (par défaut) | Oui | |

| Package logiciels | Mise à niveau possible | Conseil (si nécessaire) |
|---|---|---|
| Preview | Oui | |
| Extended | Oui | |
| 1 Previous | Non | Veuillez-vous réabonner au package « 1 Recommended ». Retrouvez plus d'informations à la section À propos de la mise à niveau de Sophos Update Manager à la page 11. |
| 1 Oldest | Non | |
| Fixed (par exemple : *1.5.4.11*) | Non | |

Si votre package logiciels n'est plus pris en charge et que vous ne changez pas d'abonnement avant la mise à niveau, le programme d'installation vous avertira de la présence d'abonnements non pris en charge. Vous ne serez pas en mesure de poursuivre la mise à niveau. Retrouvez plus d'informations sur les packages logiciels sur http://www.sophos.com/fr-fr/support/knowledgebase/112580.aspx.

## 7.1 À propos des versions fixes des logiciels

Depuis la version 5.2.1 de l'Enterprise Console, les versions fixes ne sont plus affichées dans la boîte de dialogue **Abonnement logiciels**. Si vous êtes abonné à une version fixe du logiciel et ne changez pas votre abonnement logiciels avant la mise à niveau, vous serez toujours abonné à la même version fixe après la mise à niveau et celle-ci continuera à être téléchargée. En revanche, vous ne pourrez pas vous abonner à une autre version fixe. Votre désabonnement à une version fixe entraîne sa suppression définitive de la liste des packages disponibles dans la boîte de dialogue **Abonnement logiciels**. Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/119240.aspx.

**Remarque :** depuis la version 5.2.1 de l'Enterprise Console, l'option **Mettre automatiquement à niveau la version fixe du logiciel lorsqu'elle n'est plus prise en charge par Sophos** est toujours activée et ne peut pas être désactivée. Si vous utilisez une version antérieure de l'Enterprise Console et que vous désactivez cette option dans votre abonnement logiciels, l'option sera automatiquement activée au cours de la mise à niveau et la case de la boîte de dialogue **Abonnement logiciels** disparaîtra.

## 7.2 À propos de la mise à niveau de Sophos Update Manager

Depuis la version 5.2.1, l'Enterprise Console prend uniquement en charge un seul package logiciels Sophos Update Manager identifié comme « Recommended ». Si vous procédez à la mise à niveau à partir d'une version antérieure à la version 5.2.1, le gestionnaire de mise à jour (et tous les gestionnaires de mise à jour supplémentaires que vous pourriez utiliser) doit être abonné au package « 1 Recommended ». En cas contraire, vous ne pourrez pas effectuer la mise à niveau.

Si vous n'êtes pas abonné au package « 1 Recommended », veuillez-vous y abonner et vous assurer que le Gestionnaire de mise à jour a été mis à jour à la dernière version conseillée avant de procéder à la mise à niveau de l'Enterprise Console.

Sur l'ordinateur sur lequel le serveur d'administration de l'Enterprise Console est installé, si la version du programme d'installation du Gestionnaire de mise à jour se trouvant dans le partage `\\Nomserveur\SUMInstallSet` est antérieure à la version « Recommended », le programme d'installation sera mis à jour au cours de la mise à niveau.

# 8 Téléchargement du programme d'installation

Cette section suppose que vous avez un compte MySophos et que vous avez associé vos codes d'accès de licence avec ce compte. Si vous avez besoin d'aide, consultez l'article www.sophos.com/fr-fr/support/knowledgebase/111195.aspx.

**Remarque :** vous pouvez télécharger le programme d'installation sur tout ordinateur de votre choix, puis le copier sur l'ordinateur sur lequel vous allez l'utiliser.

1. Rendez-vous sur www.sophos.com/fr-fr/support/downloads.aspx.
2. Saisissez votre nom d'utilisateur et votre mot de passe MySophos.

   Une page Web apparaît sur laquelle vos licences sont affichées.

3. Sous votre nom de licence, recherchez les téléchargements de la **Console** et téléchargez le programme d'installation de l'Enterprise Console.

# 9 Mise à niveau de l'Enterprise Console

## 9.1 Sauvegarde des données et de la configuration de l'Enterprise Console

Avant de mettre à niveau l'Enterprise Console, utilisez l'outil DataBackupRestore.exe pour sauvegarder les :

- Bases de données : Enterprise Console (principal) - SOPHOS5x, Patch - SOPHOSPATCH ou SOPHOSPATCH5x, Encryption - SOPHOSENC5x, et Auditing - SophosSecurity.
- Paramètres du registre
- Informations des comptes
- Fichiers de configuration

**Important :** l'outil DataBackupRestore.exe sauvegarde seulement la configuration du serveur d'administration Sophos depuis un emplacement d'installation par défaut. La sauvegarde ou la restauration des fichiers de configuration échoue si vous avez installé l'Enterprise Console dans un emplacement autre que celui par défaut. L'emplacement par défaut est :

- Windows 64 bits : %programfiles(x86)%\Sophos\Enterprise Console\
- Windows 32 **et** 64 bits : %programfiles%\Sophos\Enterprise Console\

Si vous utilisez un emplacement d'installation autre que celui par défaut, consultez l'article 114299 de la base de connaissances (http://www.sophos.com/fr-fr/support/knowledgebase/114299.aspx#knownissues) pour obtenir des conseils.

Si les bases de données Enterprise Console figurent sur un serveur distant, vous pouvez utiliser les outils Sophos BackupDB.bat et RestoreDB.bat pour sauvegarder et restaurer les bases de données. Retrouvez plus d'informations dans l'article 110380 de la base de connaissances du support (http://www.sophos.com/fr-fr/support/knowledgebase/110380.aspx).

Pour sauvegarder les données et la configuration de l'Enterprise Console :

1. Ouvrez une session en tant qu'administrateur sur l'ordinateur sur lequel le serveur d'administration Enterprise Console est installé.
2. Ouvrez l'Invite de commande (cliquez sur **Démarrer**, **Exécuter**, saisissez **cmd**, puis appuyez sur Entrée).
3. Naviguez jusqu'au dossier contenant l'outil.
   - Dans Windows 64 bits, saisissez :

     ```
     cd "C:\Program Files (x86)\Sophos\Enterprise Console\"
     ```

   - Dans Windows 32 bits, saisissez :

     ```
     cd "C:\Program Files\Sophos\Enterprise Console\"
     ```

4. Pour tout sauvegarder, saisissez :

   **`DataBackupRestore.exe -action=backup`**

   Pour afficher les options d'utilisation, saisissez :

   **`DataBackupRestore.exe -?`**

   Retrouvez également plus d'informations sur l'utilisation de l'outil dans l'article 114299 de la base de connaissances (http://www.sophos.com/fr-fr/support/knowledgebase/114299.aspx).

Vous êtes maintenant prêt à mettre à niveau l'Enterprise Console.

## 9.2 Mise à niveau de l'Enterprise Console

**Important :**

Si le composant Sophos Management Database est installé sur un serveur distinct, commencez par mettre à niveau le composant base de données avant de mettre à niveau le serveur d'administration.

Ne modifiez pas l'Enterprise Console (par exemple, changer les paramètres des stratégies) entre la mise à niveau de la base de données et la mise à niveau du serveur d'administration.

Retrouvez plus d'informations sur la mise à niveau de la base de données sur un serveur distant, sur la mise à niveau sur un serveur sécurisé à l'aide d'un script et sur la mise à niveau dans un environnement SQL Server en cluster dans l'article 33980 de la base de connaissances du support de Sophos (http://www.sophos.com/fr-fr/support/knowledgebase/33980.aspx).

Pour mettre à niveau l'Enterprise Console :

1. Sur l'ordinateur sur lequel vous souhaitez mettre à niveau l'Enterprise Console, ouvrez une session avec les droits administrateur.
   - Si le serveur est dans un domaine, utilisez un compte de domaine disposant des droits d'administrateur local.
   - Si le serveur est dans un groupe de travail, utilisez un compte local disposant des droits d'administrateur local.
2. Recherchez le programme d'installation de l'Enterprise Console que vous avez téléchargé auparavant.

   **Info :** le nom de fichier du programme d'installation inclut le mot « sec ».
3. Cliquez deux fois sur le programme d'installation.
4. Un assistant vous guide tout au long de la mise à niveau.
5. Si vous procédez à la mise à niveau à partir de l'Enterprise Console 5.0 et souhaitez ajouter Sophos Disk Encryption :
   a) Sur la page **Administration du chiffrement** de l'assistant, sélectionnez **Administrer le chiffrement**.
   b) Sur la page **Chiffrement Sophos**, cliquez sur **Nouvelles installations**. Vous êtes invité à créer un mot de passe pour le magasin de sauvegarde des certificats. Notez le mot de passe.
6. Fermez l'assistant.

Si vous procédez à la mise à niveau à partir de l'Enterprise Console 5.1 et souhaitez ajouter Sophos Disk Encryption, exécutez de nouveau le programme d'installation de l'Enterprise

Console 5.3.0. Le programme d'installation affiche désormais les options d'administration du chiffrement comme décrit à l'étape 5 ci-dessus.

Après avoir ajouté le chiffrement, vous allez devoir installé le logiciel de chiffrement sur les ordinateurs d'extrémité comme décrit à la section Annexe B : installation du logiciel de chiffrement sur les ordinateurs d'extrémité à la page 19.

**Important :** la nouvelle base de données d'audit de Sophos appelée **SophosSecurity** doit être présente et s'exécuter en même temps que les autres bases de données de l'Enterprise Console même si vous n'avez pas l'intention d'utiliser la fonction d'audit de Sophos. En effet, cette base de données est utilisée pour les événements de contrôle d'accès renforcé et de journalisation des audits.

## 9.3 Renforcement de la sécurité de la base de données

### Audit de la base de données

En plus de la protection intégrée aux bases de données Enterprise Console, nous vous conseillons de paramétrer la protection supplémentaire au niveau de l'instance SQL Server (s'il n'est pas déjà en place) pour auditer les activités de l'utilisateur et les modifications qu'il a effectué sur votre SQL Server.

Par exemple, si vous utilisez une édition Enterprise de SQL Server 2008, vous pouvez utiliser la fonction SQL Server Audit. Des versions précédentes de SQL Server prennent en charge l'audit de connexion, l'audit par déclencheur externe et l'audit des événements à l'aide d'un utilitaire de suivi intégré.

Retrouvez plus d'informations sur les fonctions que vous pouvez utiliser pour procéder à l'audit des activités et des modifications sur votre système SQL Server dans la documentation correspondant à votre version de SQL Server. Par exemple :

- SQL Server Audit (moteur de base de données)
- Audit (moteur de base de données), SQL Server 2008 R2
- Audit dans SQL Server 2008
- Audit (moteur de base de données), SQL Server 2008

### Chiffrement des connexions à la base de données

Nous vous conseillons fortement de chiffrer les connexions entre tous les clients et la base de données Enterprise Console. Retrouvez plus d'informations dans la documentation de SQL Server :

- Activer les connexions chiffrées dans le moteur de base de données (Gestionnaire de configuration SQL Server)
- Chiffrement des connexions à SQL Server 2008 R2
- Comment faire pour activer le chiffrement SSL pour une instance de SQL Server à l'aide de la console MMC

### Contrôle de l'accès aux copies de sauvegardes de la base de données

Assurez-vous qu'un contrôle d'accès correct et restrictif aux copies de sauvegarde de la base de données est mis en place. Ceci permet de garantir que les utilisateurs non autorisés n'auront pas accès aux fichiers, ne pourront pas les altérer ou les supprimer accidentellement.

**Remarque :** les liens de cette section vous dirigent vers des informations mises à jour par des tiers et sont fournies pour vous aider. Même si nous vérifions régulièrement l'exactitude de ces liens, il se peut que ceux-ci soient modifiés sans que nous en ayons connaissance.

## 9.4 Vérification des stratégies existantes

### 9.4.1 Vérification des paramètres de stratégie

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour réaliser ces tâches. Retrouvez plus d'informations à la rubrique « À propos des rôles et des sous-parcs » de la section « Gestion des rôles et des sous-parcs » dans l'*Aide de Sophos Enterprise Console*.

Pour vous assurer que les paramètres de la stratégie ont été préservés suite à la mise à niveau de l'Enterprise Console :

1. Démarrez l'Enterprise Console.
2. Dans le volet **Stratégies**, cliquez deux fois sur un type de stratégie (par exemple, **Antivirus et HIPS**).
3. Cliquez deux fois sur la stratégie que vous désirez vérifier.
4. Dans la boîte de dialogue qui apparaît, vérifiez les paramètres de la stratégie.

### 9.4.2 Vérification des stratégies appliquées aux groupes d'ordinateurs

**Remarque :** si vous utilisez l'administration déléguée, vous devez disposer du droit **Recherche d'ordinateurs, protection et groupes** pour réaliser ces tâches. Retrouvez plus d'informations à la rubrique « À propos des rôles et des sous-parcs » de la section « Gestion des rôles et des sous-parcs » dans l'*Aide de Sophos Enterprise Console*.

Pour vérifier que les stratégies appliquées aux groupes sont correctes suite à la mise à niveau de l'Enterprise Console, procédez de la manière suivante :

**Remarque :** les fonctions qui ne sont pas incluses dans votre licence et qui étaient disponibles dans les anciennes versions de l'Enterprise Console ne seront plus disponibles.

1. Démarrez l'Enterprise Console.
2. Dans le volet **Groupes**, cliquez avec le bouton droit de la souris sur un groupe et cliquez sur **Voir/Modifier les détails de la stratégie du groupe**.
3. Dans la boîte de dialogue **Détails du groupe**, assurez-vous que les stratégies affectées au groupe sont correctes. Si elles ne le sont pas, sélectionnez une stratégie différente dans la liste déroulante.

La mise à niveau de l'Enterprise Console est maintenant terminée.

Retrouvez plus d'informations sur l'installation du logiciel de chiffrement sur les ordinateurs d'extrémité dans l'Annexe B : installation du logiciel de chiffrement sur les ordinateurs d'extrémité à la page 19.

# 10 Activation de la détection du trafic malveillant

La version 5.3.0 de l'Enterprise Console offre l'option de Détection du trafic malveillant pour détecter les communications entre les ordinateurs d'extrémité et les serveurs de commande et de contrôle impliqués dans les attaques par botnet ou par autre programme malveillant. Pour bénéficier de cette fonction, vous devez l'activer suite à la mise à niveau.

**Remarque :** la détection du trafic malveillant est actuellement uniquement compatible avec des systèmes d'exploitation non serveur Windows 7 et supérieur et elle est disponible à partir de la version 10.6.0 d'Endpoint Security and Control.

1. Vérifiez quelle stratégie antivirus et HIPS est utilisée par le ou les groupes d'ordinateurs sur lesquels vous voulez activer cette nouvelle fonction.

   Dans le volet **Groupes**, cliquez avec le bouton droit de la souris sur le groupe. Sélectionnez **Voir/Modifier les détails de la stratégie du groupe**. Dans la boîte de dialogue des détails du groupe apparaissent les stratégies en cours d'utilisation.

2. Dans le volet **Stratégies**, cliquez deux fois sur **Antivirus et HIPS**.
3. Cliquez deux fois sur la stratégie que vous désirez modifier.

   La boîte de dialogue **Stratégie antivirus et HIPS** apparaît.

4. Dans le volet **Contrôle sur accès**, assurez-vous que la case à cocher **Activer la surveillance des comportements** est sélectionnée.
5. À côté de **Activer la surveillance des comportements**, cliquez sur **Configurer**.
6. Dans la boîte de dialogue **Configuration de la surveillance des comportements**, assurez-vous que la case **Détecter les comportements malveillants** est sélectionnée.
7. Pour activer la détection du trafic malveillant, sélectionnez la case **Détecter le trafic malveillant**.

   **Remarque :** la détection du trafic malveillant utilise la même série d'exclusions que le contrôle sur accès de Sophos Anti-Virus.

# 11 Annexes

## 11.1 Annexe A : mise à niveau de Sophos Disk Encryption 5.61 vers SafeGuard Enterprise

La migration de Sophos Disk Encryption 5.61 vers SafeGuard Enterprise nécessite d'effectuer les étapes suivantes :

- Exportation du certificat d'entreprise de SEC : Dans le menu **Outils** de l'Enterprise Console, cliquez sur **Gérer le chiffrement** et sélectionnez **Sauvegarde du certificat d'entreprise**. Sélectionnez un répertoire de destination et un nom de fichier, puis saisissez un mot de passe pour le fichier .P12 lorsque vous y êtes invité.
- Installez SafeGuard Management Center et SafeGuard Enterprise Server.

  **Remarque :** si vous avez installé le serveur d'administration SEC avec le chiffrement sur ce serveur, installez SafeGuard Enterprise sur un serveur différent.

- Dans l'assistant de configuration de SafeGuard Management Center, sélectionnez une nouvelle base de données à créer et importez le certificat d'entreprise exporté auparavant.
- Dans SafeGuard Management Center, créez le package de configuration des ordinateurs d'extrémité : Dans le menu **Outils**, cliquez sur **Outil du package de configuration**. Sélectionnez **Packages client administrés**, effectuez vos changements et créez le package de configuration.
- Déployez le package de configuration sur les ordinateurs d'extrémité. Une fois que les ordinateurs d'extrémité l'ont reçu, ils peuvent se connecter au serveur SafeGuard Enterprise. À partir de ce moment-là, l'ordinateur d'extrémité peut être administré par SafeGuard Management Center.
- Dans SafeGuard Management Center, créez et attribuez des stratégies comme vous le souhaitez.

Les ordinateurs d'extrémité migrés restent visibles dans l'Enterprise Console sous l'état « administrés par SafeGuard Enterprise ». Il est toujours possible d'effectuer toutes les tâches non associées au chiffrement sur ces ordinateurs.

Retrouvez plus d'informations détaillées sur l'installation de SafeGuard Enterprise dans le *Guide d'installation de SafeGuard Enterprise*.

## 11.2 Annexe B : installation du logiciel de chiffrement sur les ordinateurs d'extrémité

Lisez cette section si :

- Votre licence inclut le chiffrement.
- Vous n'utilisez pas actuellement le chiffrement Sophos.
- Vous avez installé l'Enterprise Console pour gérer le chiffrement.

**Attention ! Lorsque vous installez le logiciel de chiffrement de Sophos pour la première fois, nous vous conseillons fortement d'activer et de tester chaque paramètre l'un après l'autre.**

Pour paramétrer le chiffrement intégral du disque sur les ordinateurs, vous devez :

- Vous abonner au logiciel de chiffrement.
- Préparer l'installation du logiciel de chiffrement.
- Installer automatiquement le logiciel de chiffrement.
- Installer manuellement le logiciel de chiffrement.

**Remarque :** le chiffrement intégral du disque peut être installé sur les ordinateurs Windows XP, Windows Vista et Windows 7 mais pas sur les ordinateurs Windows 8 ou supérieur ni sur les Mac.

**Attention !** Avant d'installer le chiffrement intégral du disque sur les ordinateurs :

- Assurez-vous que les lecteurs chiffrés avec le logiciel de chiffrement tiers ont été déchiffrés et que ce logiciel de chiffrement tiers est désinstallé.
- Créez une sauvegarde complète des données sur les ordinateurs.

Retrouvez une liste complète des préparations à la section Préparation des ordinateurs à l'installation à la page 22.

### 11.2.1 Abonnement au logiciel de chiffrement

**Remarque :** nous vous conseillons de créer un nouvel abonnement pour le chiffrement.

Pour vous abonner au logiciel de chiffrement :

1. Dans l'Enterprise Console, dans le menu **Affichage**, cliquez sur **Gestionnaires de mise à jour**.
2. Pour créer un nouvel abonnement, dans le volet **Abonnements logiciels**, cliquez sur le bouton **Ajouter** en haut du volet. Dans la boîte de dialogue **Abonnement logiciels**, saisissez un nom pour cet abonnement dans la boîte **Nom de l'abonnement**. Sous **Produits de chiffrement**, près de **Windows XP and above**, cliquez dans la case **Version** et sélectionnez la dernière version « Recommended » (version 5.61 à l'heure de cette publication). Cliquez sur **OK**.
3. Pour ajouter l'abonnement aux **Gestionnaires de mise à jour**, dans le volet **Gestionnaires de mise à jour**, cliquez avec le bouton droit de la souris sur le gestionnaire de mise à jour et sélectionnez **Voir/Modifier la configuration**. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Abonnements**, sélectionnez l'abonnement dans la liste **Disponible** et cliquez sur le bouton > pour le déplacer dans la liste **Abonné à**. Cliquez sur **OK**.

Le logiciel de chiffrement est téléchargé dans le partage par défaut \\<nom_serveur>\SophosUpdate\CIDs\<abonnement>\ENCRYPTION.

Pour télécharger sur des partages autres que le partage par défaut, reportez-vous à la section Indication de l'emplacement du logiciel à la page 21.

Pour modifier la planification des mises à jour par défaut, reportez-vous à la section Modification d'une planification des mises à jour à la page 21.

**Remarque :** l'application des stratégies de mise à jour à un groupe d'ordinateurs n'installe pas le logiciel de chiffrement. Vous devez lancer l'installation du logiciel de chiffrement vous-même.

Retrouvez plus d'informations sur la stratégie de chiffrement intégral du disque dans le *Guide de configuration des stratégies de l'Enterprise Console*.

### 11.2.2 Indication de l'emplacement du logiciel

Après avoir sélectionné le logiciel à télécharger, vous pouvez indiquer où il doit être placé sur le réseau. Par défaut, le logiciel est placé dans un partage UNC `\\<NomOrdinateur>\SophosUpdate`, où NomOrdinateur est le nom de l'ordinateur sur lequel le gestionnaire de mise à jour est installé.

Vous pouvez distribuer le logiciel téléchargé sur les partages supplémentaires de votre réseau. Pour cela, ajoutez un partage réseau existant dans la liste des partages disponibles, puis déplacez-le dans la liste des partages de mise à jour comme décrit ci-dessous.

Pour indiquer où le logiciel est placé :

1. Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Distribution**, sélectionnez un abonnement logiciels dans la liste.
2. Sélectionnez un partage dans la liste des partages « Disponibles » et déplacez-le dans la liste « Mettre à jour dans » en cliquant sur le bouton **>**.

   Le partage par défaut `\\<NomOrdinateur>\SophosUpdate` est toujours présent dans la liste « Mettre à jour dans ». Vous ne pouvez pas supprimer ce partage de la liste.

   La liste des partages « Disponibles » inclut tous les partages connus par l'Enterprise Console et qui ne sont pas déjà utilisés par un autre gestionnaire de mise à jour.

   Vous pouvez ajouter un partage existant dans la liste des partages « Disponibles » ou en enlever un à l'aide du bouton **Ajouter** ou **Supprimer**.

3. Si vous voulez saisir une description de partage ou les codes d'accès nécessaires pour écrire dans le partage, sélectionnez ce dernier et cliquez sur **Configurer**.
4. Dans la boîte de dialogue **Gestionnaire des partages**, saisissez la description et les codes d'accès.

Le logiciel que vous avez sélectionné sera téléchargé dans les partages que vous avez indiqués à la prochaine mise à jour planifiée.

Si vous voulez modifier la planification des mises à jour par défaut, reportez-vous à la section Modification d'une planification des mises à jour à la page 21.

Si vous voulez télécharger les logiciels immédiatement, sélectionnez le gestionnaire de mise à jour, cliquez avec le bouton droit de la souris et cliquez sur **Mettre à jour maintenant**.

### 11.2.3 Modification d'une planification des mises à jour

Par défaut, un gestionnaire de mise à jour vérifie les mises à jour des données de détection des menaces toutes les 10 minutes. Vous pouvez changer cet intervalle de mise à jour. La valeur minimum est 5 minutes. La valeur maximum est 1440 minutes (24 heures). Sophos conseille de choisir un intervalle de mise à jour de 10 minutes pour les données de détection des menaces pour que vous receviez une protection contre les nouvelles menaces immédiatement après la publication par Sophos de ces données de détection.

Par défaut, un gestionnaire de mise à jour vérifie les mises à jour des logiciels toutes les 60 minutes. Vous pouvez changer cet intervalle de mise à jour. La valeur minimum est 10 minutes. La valeur maximum est 1440 minutes (24 heures).

Pour les mises à jour logicielles, vous pouvez soit spécifier un intervalle de mise à jour utilisé toutes les heures chaque jour, soit créer des planifications plus sophistiquées où chaque jour

peut être défini indépendamment et divisé en périodes avec des intervalles de mise à jour différents.

**Remarque :** vous pouvez créer une planification différente pour chaque jour de la semaine. Seule une planification peut être associée à un jour de la semaine.

Si vous voulez changer la planification par défaut :

- Dans la boîte de dialogue **Configuration du gestionnaire de mise à jour**, sur l'onglet **Planification**, saisissez les nouveaux intervalles de mise à jour ou créez une planification plus détaillée, ou encore des planifications différentes suivant les jours de la semaine.

Si vous le souhaitez, vous pouvez aussi changer les paramètres par défaut du journal et de la mise à jour automatique du gestionnaire de mise à jour. Exécutez cette opération en modifiant les paramètres respectivement dans les onglets **Journalisation** et **Avancés**.

## 11.2.4 Préparation de l'installation du logiciel de chiffrement

La préparation de l'installation du logiciel de chiffrement sur les ordinateurs implique les tâches suivantes :

- Attribuer aux administrateurs l'accès aux ordinateurs suite à l'installation.
- Préparer les ordinateurs à l'installation.

### 11.2.4.1 Attribution de l'accès administrateur aux ordinateurs suite à l'installation

Les administrateurs peuvent avoir besoin d'accéder et de préconfigurer les ordinateurs après avoir installé le logiciel de chiffrement, par exemple pour installer d'autres logiciels. Toutefois, le premier utilisateur qui se connecte après l'installation active l'authentification au démarrage.

Pour éviter ceci, ajoutez les administrateurs respectifs à la liste des exceptions comme suit :

1. Dans le volet **Stratégies** de l'Enterprise Console, cliquez deux fois sur **Chiffrement intégral du disque**. Cliquez deux fois sur la stratégie **Par défaut** pour la modifier.
2. Sous **Authentification au démarrage (POA)**, cliquez sur **Exceptions** près de **Activer l'authentification au démarrage**.
3. Dans **Exceptions**, cliquez sur **Ajouter**, saisissez le **Nom d'utilisateur** et le **Nom de l'ordinateur ou de domaine** du ou des comptes Windows correspondants et cliquez sur **OK**.

   Vous pouvez utiliser des caractères génériques comme premier ou dernier caractère. Dans le champ **Nom d'utilisateur**, le caractère ? n'est pas autorisé. Dans le champ **Nom de l'ordinateur ou de domaine**, les caractères / \ [ ] : ; | = , + ? < > " ne sont pas autorisés.
4. Dans la boîte de dialogue des stratégies **Par défaut**, cliquez sur **OK**.
5. Dans le volet **Stratégies**, sélectionnez la stratégie et déplacez-la sur le groupe auquel vous voulez appliquer la stratégie. Lorsque vous y êtes invité, confirmez si vous désirez continuer.

### 11.2.4.2 Préparation des ordinateurs à l'installation

Si votre licence inclut le chiffrement intégral du disque, effectuez d'abord les étapes suivantes avant d'installer le logiciel de chiffrement sur les ordinateurs :

- Assurez-vous que les lecteurs chiffrés avec le logiciel de chiffrement tiers ont été déchiffrés et que ce logiciel de chiffrement tiers est désinstallé.
- Créez une sauvegarde complète des données.

- Vérifiez si un compte utilisateur Windows avec codes d'accès est configuré et actif sur l'ordinateur d'extrémité.
- Avant de déployer le chiffrement intégral du disque, assurez-vous que l'ordinateur a déjà été protégé avec la version 10 du logiciel antivirus Sophos.
- Désinstallez les gestionnaires de démarrage tiers, tels que PROnetworks Boot Pro et Boot-US.
- Créez une sauvegarde complète des données.
- Recherchez toutes les erreurs du ou des disques durs à l'aide de cette commande :

  **`chkdsk %drive% /F /V /X`**

  Il se peut que vous soyez invité à redémarrer votre ordinateur et à exécuter de nouveau la commande **`chkdsk`**. Retrouvez plus d'informations sur : http://www.sophos.com/fr-fr/support/knowledgebase/107799.aspx.

  Vous pouvez vérifier les résultats (fichier journal) dans l'Observateur d'événements Windows :

  Windows XP : sélectionnez **Application**, **Winlogon**.
  Windows 7, Windows Vista : sélectionnez **Journaux Windows**, **Application**, **Wininit**.

- Utilisez l'outil de défragmentation intégré de Windows appelé **`defrag`** pour localiser et consolider les fichiers de démarrage, les fichiers de données et les dossiers fragmentés sur les lecteurs locaux :

  **`defrag %drive%`**

  Retrouvez plus d'informations sur : http://www.sophos.com/fr-fr/support/knowledgebase/109226.aspx.

- Si vous avez utilisé un outil d'image/de clone sur l'ordinateur, nettoyez l'enregistrement de démarrage principal (MBR, master boot record). Démarrez l'ordinateur à partir d'un DVD Windows et utilisez la commande **`FIXMBR`** dans la Console de récupération Windows. Retrouvez plus d'informations sur : http://www.sophos.com/fr-fr/support/knowledgebase/108088.aspx.
- Si la partition de démarrage de l'ordinateur a été convertie du format FAT au format NTFS et si l'ordinateur n'a pas encore été redémarré, redémarrez l'ordinateur. Si vous ne faites pas cela, il est possible que l'installation ne s'effectue pas avec succès.
- Ouvrez le Pare-feu Windows avec fonctions avancées de sécurité en allant dans le Panneau de configuration et en cliquant sur **Outils d'administration**. Assurez-vous que les **Connexions entrantes** sont autorisées. Changez les **Règles de trafic entrant** pour activer les processus ci-dessous.

  Administration à distance (NP-Entrée) Domaine
  Administration à distance (NP-Entrée) Privé
  Administration à distance (RPC) Domaine
  Administration à distance (RPC) Privé
  Administration à distance (RPC-EPMAP) Domaine
  Administration à distance (RPC-EPMAP) Privé

  Lorsque l'installation est terminée et si vous souhaitez continuer à utiliser le pare-feu Windows, vous pouvez désactiver le processus.

### 11.2.5 Installation automatique du logiciel de chiffrement

**Attention ! Si vous installez le logiciel de chiffrement de Sophos pour la première fois, nous vous conseillons fortement d'activer et de tester chaque paramètre l'un après l'autre.**

Assurez-vous que les ordinateurs d'extrémité ont été préparés pour l'installation du chiffrement intégral du disque, mais surtout que le logiciel de chiffrement tiers a été désinstallé, que toutes les données ont été sauvegardées et que la version 10 du logiciel antivirus de Sophos a été installée.

Pour installer le logiciel de chiffrement automatiquement :

1. Dans l'Enterprise Console, sélectionnez les ordinateurs sur lesquels vous voulez installer le chiffrement intégral du disque.
2. Cliquez avec le bouton droit de la souris sur l'ordinateur, puis cliquez sur **Protéger les ordinateurs**. L'**Assistant de protection des ordinateurs** est lancé.
3. Sur la page **Bienvenue**, cliquez sur **Suivant**.
4. Sur la page **Type d'installation**, sélectionnez **Logiciel de chiffrement**.
5. Si plus d'un abonnement au chiffrement et plus d'un emplacement du programme d'installation (emplacement du fichier d'amorce) sont disponibles, la page **Emplacement du chiffrement** apparaît. Sélectionnez l'**Abonnement au chiffrement** et l'**Adresse** à partir de laquelle effectuer l'installation.
6. Sur la page **Récapitulatif du chiffrement**, vérifiez tous les problèmes d'installation.
7. Sur la page **Codes d'accès**, saisissez les détails d'un compte qui peut être utilisé pour installer le logiciel sur les ordinateurs.

L'installation s'effectue par étapes. Aussi, l'opération peut prendre un certain temps avant de se terminer sur tous les ordinateurs.

Les ordinateurs vont redémarrer automatiquement dans les 30 minutes suivant l'installation du logiciel de chiffrement. Si le chiffrement est activé par une stratégie, il sera appliqué uniquement après le redémarrage de l'ordinateur.

Retrouvez plus d'informations sur le comportement de l'ordinateur au démarrage et à la première connexion suite à l'installation et à l'activation du chiffrement à la section Première connexion après installation à la page 25.

### 11.2.6 Installation manuelle du logiciel de chiffrement

**Attention ! Si vous installez le logiciel de chiffrement de Sophos pour la première fois, nous vous conseillons fortement d'activer et de tester chaque paramètre l'un après l'autre.**

S'il est impossible de protéger automatiquement certains de vos ordinateurs, protégez-les en exécutant un programme d'installation depuis le dossier partagé dans lequel le logiciel de chiffrement a été téléchargé. Ce dossier partagé est plus connu sous le nom d'*emplacement du fichier d'amorce*.

Assurez-vous que les ordinateurs d'extrémité ont été préparés pour l'installation du chiffrement intégral du disque, mais surtout que le logiciel de chiffrement tiers a été désinstallé, que toutes les données ont été sauvegardées et que la version 10 du logiciel antivirus de Sophos a été installée.

Lors de l'installation du chiffrement intégral du disque, assurez-vous qu'il n'y a qu'une seule session utilisateur active sur l'ordinateur d'extrémité. Si vous n'effectuez pas cette opération, l'installation échouera.

Ouvrez une session en tant qu'administrateur Windows sur les ordinateurs que vous voulez protéger.

Pour installer manuellement le logiciel de chiffrement sur les ordinateurs :

1. Pour savoir dans quel répertoire se trouve le programme d'installation, ouvrez l'Enterprise Console et sélectionnez **Emplacements des fichiers d'amorce** dans le menu **Affichage**.

   Dans la boîte de dialogue **Emplacements des fichiers d'amorce**, la colonne **Emplacement** affiche le chemin de l'emplacement des fichiers d'amorce pour chaque plate-forme. Notez le nom des chemins concernés.

2. Sur l'ordinateur qui héberge l'emplacement du fichier d'amorce, créez un compte utilisateur en lecture seule.
3. Allez sur chaque ordinateur et connectez-vous avec les droits d'administrateur local.
4. Recherchez le programme de configuration du chiffrement setup.exe dans l'emplacement du fichier d'amorce et cliquez deux fois dessus.

   Le programme de configuration du chiffrement est disponible à l'emplacement suivant : \\<NomServeur>\SophosUpdate\CIDs\<Subscription>\ENCRYPTION

5. Un assistant vous guide tout au long de l'installation du logiciel de chiffrement.

Retrouvez plus d'informations sur le comportement de l'ordinateur au démarrage et à la première connexion suite à l'installation et à l'activation du chiffrement à la section Première connexion après installation à la page 25.

## 11.2.7 Première connexion après installation

Après l'installation du chiffrement, l'ordinateur redémarre et l'utilisateur est invité à se connecter. Le comportement de l'ordinateur dépend du type de compte avec lequel l'utilisateur se connecte :

- Connexion en tant qu'utilisateur avec un compte Windows normal.
- Connexion pour tâches administratives avec un compte Windows répertorié sur une liste d'exceptions.

### Connexion en tant qu'utilisateur avec un compte Windows normal

La procédure de connexion correspond seulement à celle décrite ici si l'authentification au démarrage et le chiffrement ont été activés dans la stratégie de chiffrement intégral du disque.

Lorsque l'ordinateur redémarre, un certain nombre de messages (par exemple, l'écran de connexion automatique) s'affichent. Ensuite, le système d'exploitation Windows démarre. L'utilisateur se connecte à Windows à l'aide de ses codes d'accès Windows. L'utilisateur est enregistré en tant qu'utilisateur Sophos SafeGuard sur l'ordinateur.

**Remarque :** pour confirmer le succès de l'enregistrement, une infobulle apparaît sur l'ordinateur d'extrémité.

S'il est activé par la stratégie, le chiffrement démarre sur les lecteurs sélectionnés. Le chiffrement et le déchiffrement sont exécutés en tâches de fond sans intervention de l'utilisateur. L'utilisateur peut continuer de travailler ou éteindre l'ordinateur pendant le processus de chiffrement. Aucun redémarrage n'est requis suite à l'installation du chiffrement.

L'authentification au démarrage sera activée la prochaine fois que l'utilisateur démarrera l'ordinateur. Désormais, l'utilisateur a uniquement besoin de saisir ses codes d'accès Windows à l'authentification au démarrage pour se connecter automatiquement à Windows.

**Remarque :** lors du démarrage de l'ordinateur après mise en veille, l'utilisateur doit saisir ses codes d'accès Windows à l'authentification au démarrage et dans Windows.

Retrouvez plus d'informations dans le *Manuel d'utilisation de Sophos Disk Encryption.*

## Connexion pour tâches administratives avec un compte Windows répertorié sur une liste d'exceptions

La procédure de connexion correspond seulement à celle décrite ici si l'utilisateur se connecte à un compte Windows qui a été placé dans une liste d'exceptions et si l'authentification au démarrage a été activée dans la stratégie de chiffrement intégral du disque.

Lorsque l'ordinateur redémarre, le système d'exploitation Windows démarre. La boîte de dialogue de connexion Windows apparaît. L'utilisateur se connecte à l'aide de ses codes d'accès définis auparavant dans la stratégie de chiffrement intégral du disque. L'utilisateur est connecté à Windows en tant qu'utilisateur invité. L'authentification au démarrage n'est pas activée. Le processus de chiffrement ne démarre pas. L'utilisateur peut procéder aux tâches postérieures à l'installation nécessaires.

# 12 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur www.sophos.com/fr-fr/support.aspx.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation.aspx.
- Ouvrez un incident support sur https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx.

# 13 Mentions légales

Copyright © 2013–2015 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos, Sophos Anti-Virus et SafeGuard sont des marques déposées de Sophos Limited, Sophos Group et de Utimaco Safeware AG, partout ou ceci est applicable. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

## ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us know so we can promote your project in the DOC software success stories.

The ACE, TAO, CIAO, DAnCE, and CoSMIC web sites are maintained by the DOC Group at the Institute for Software Integrated Systems (ISIS) and the Center for Distributed Object Computing of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies around the world provide

commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

## Apache

Les logiciels Sophos mentionnés dans le présent document peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Apache. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur http://www.apache.org/licenses/LICENSE-2.0.

## Boost

Version 1.0, 17 August 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the “Software”) to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Common Public License

Les logiciels Sophos auxquels le présent document fait référence incluent ou peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Common Public License (CPL), qui, entre autres droits, permettent à l'utilisateur d'avoir accès au code source. La licence CPL exige que pour tout logiciel concédé

en licence sous les termes de la licence CPL, qui est distribuée sous un format de code objet, le code source soit aussi mis à disposition de ces utilisateurs sous un format de code objet. Pour chaque logiciel couvert par la licence CPL, le code source est disponible sur commande par courrier postal envoyé à Sophos, par e-mail à support@sophos.fr ou par Internet sur http://www.sophos.com/fr-fr/support/contact-support/contact-information.aspx. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur http://opensource.org/licenses/cpl1.0.php

## ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

## Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

**OpenSSL license**

Copyright © 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

**Original SSLeay license**

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

   The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

## WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.